Auditdienst Rijk
Ministerie van Financiën

Assurancerapport
Wpg hercontrole Douane

Definitief

Colofon

Titel	Wpg hercontrole Douane
Uitgebracht aan	Douane
Datum	26 februari 2024
Kenmerk	

Inlichtingen
Auditdienst Rijk

Inhoud

1 Inleiding

1.1 Aanleiding

De Wet Politiegegevens (Wpg) is sinds 2007 van toepassing verklaard op de verwerking van persoonsgegevens die in het kader van de politietaak worden verwerkt. Naar aanleiding van de inwerkingtreding van de Richtlijn (EU) 2016/680 in 2016 is de Wpg in 2019 aangepast en is het Besluit politiegegevens buitengewoon opsporingsambtenaar (Bpg boa) in werking getreden. Vanaf dat moment vallen buitengewone opsporingsambtenaren (boa's) die voor hun opsporingstaak persoonsgegevens verwerken onder de Wpg. De Wpg is daarmee van toepassing op de taken van de Douane.

De Regeling periodieke audit politiegegevens schrijft voor dat de verwerkingsverantwoordelijke de naleving van de regels gesteld in de Wpg controleert door middel van periodieke audits, zowel intern als extern. Werkgevers van boa's zijn verplicht om elk jaar een interne Wpg-audit te doen en elke 4 jaar een externe Wpg-audit (hierna Privacy audit). Het resultaat van de Privacy audit moet worden gedeeld met de Autoriteit Persoonsgegevens (AP) als de bij wet aangestelde toezichthouder in Nederland.

De Wpg bepaalt dat de eerste Privacy audit twee jaar na inwerkintreding moet worden uitgevoerd. De auditverplichting is met ingang van 01-01-2019 van kracht geworden voor (de werkgevers van) boa's. In april 2022 is door de Auditdienst Rijk (ADR) een Privacy audit uitgevoerd (kenmerk 2022-0000310180). De resultaten van deze audit zijn door de Douane gedeeld met de AP. De rapportage leidde tot een groot aantal bevindingen die middels een verbetertraject door de Douane zijn opgepakt. Het opgestelde verbeterplan heeft de uitvoering van de aanbevelingen over de kwartalen 2, 3, en 4 van 2023 en het eerste kwartaal van 2024 verspreid. Deze hercontrole zag op de voortgang op de aanbevelingen uit kwartalen 2 en 3 van 2023.

Door de Douane is aan de ADR gevraagd om de uitkomsten van het verbetertraject uit de kwartalen 2 en 3 voor de geselecteerde bevindingen te beoordelen. Tijdens de beoordeling zijn alleen de normen onderzocht waarop aantoonbare voortgang is geboekt. Het uitvoeren van deze hercontrole is een wettelijke verplichting waarbij de verwerkingsverantwoordelijke een afschrift van de (her)controleresultaten aan de AP dient te zenden.

De Douane is verantwoordelijk voor de opzet en het bestaan van de aanvullende beheersingsmaatregelen om alsnog te kunnen voldoen aan het bij of krachtens de Wpg bepaalde, binnen een jaar na de initiële externe privacy audit[1].

1.2 Context

De Nederlandse Douane heeft verschillende taken en bevoegdheden op het gebied van fiscaliteit, maar ook van veiligheid, gezondheid, economie en milieu (afgekort als VGEM). De Douane houdt hiervoor bijvoorbeeld toezicht op de invoer, de uitvoer en het vervoer van goederen.

[1] Artikel 33 Wet politiegegevens en Artikel 4 Regeling periodieke audit politiegegevens.

Daarbij controleert de Douane of de bij invoer en uitvoer verschuldigde belastingen worden betaald en of goederen bij uitvoer voldoen aan de voorschriften.

Daarnaast ziet de Douane toe op de naleving van wetgeving op het gebied van Veiligheid, Gezondheid, Economie en Milieu, VGEM. Deze wetgeving schrijft voor dat invoer, uitvoer of vervoer van bepaalde goederen in Nederland en/of de Europese Unie verboden is, of alleen is toegestaan als wordt voldaan aan (strenge) voorwaarden, of als de goederen aan bepaalde eisen voldoen. Vanwege de VGEM-taken voert de Douane een groot aantal controlerende, signalerende en opsporingstaken uit in opdracht van verschillende ministeries.

Daarnaast kan de douanemedewerker ook buitengewoon opsporingsambtenaar zijn. Deze opsporingsbevoegdheid gebruikt de douanemedewerker als hij bij zijn controletaken overtredingen tegenkomt en strafbare feiten vermoedt en/of vaststelt. In scope van deze opdracht zijn de taken die door de boa's in het kader van opsporing worden uitgevoerd. Deze verwerking in het kader van opsporingstaken valt onder de Wpg.

Wanneer onregelmatigheden worden aangetroffen die strafbaar zijn gesteld kan het voorkomen dat de douanemedewerker gebruik moet maken van opsporingsbevoegdheden. De douanemedewerker kan bevoegdheden in de opsporingssfeer toepassen wanneer men beschikt over een aanwijzing als buitengewoon opsporingsambtenaar (boa). Voor de Douane geldt dat de verwerking van persoonsgegevens in het kader van boa-werkzaamheden, zoals het opmaken van een proces-verbaal (PV) na het constateren van een strafbaar feit (conform de Algemene Douanewet de AWR of andere wetgeving) of het opleggen van een Fiscale Strafbeschikking (FSB) vallen onder de reikwijdte van de Wet politiegegevens en het Besluit politiegegevens boa (Bpg boa).

De Wpg en het bijbehorende Bpg boa zorgen voor een evenwicht tussen de belangen die met de politietaak gemoeid zijn en de bescherming van de privacy van de burger.

2 Oordelen en bevindingen hercontrole

2.1 De Douane heeft op een aantal onderdelen verbeteringen gerealiseerd echter nog niet op alle onderwerpen zijn verbeteringen in gang gezet

Wij hebben de beheersingsmaatregelen, welke bij de initiële privacy audit zijn beoordeeld als 'voldoet deels' of 'voldoet niet' én waarvan de organisatie heeft aangegeven verbeteringen te hebben gerealiseerd van materieel belang, opnieuw beoordeeld. Naar ons oordeel zijn de algehele beheersingsmaatregelen om te voorzien in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens door boa's door de Douane niet op afdoende wijze in opzet en bestaan ingevuld. De Douane voldoet hiermee, ondanks gerealiseerde verbetermaatregelen op een aantal onderwerpen, niet aan de Wpg.

Wanneer in het licht van de gehele eerdere uitgevoerde audit wordt gekeken, is te zien dat het opgestelde verbeterplan tot het wegwerken van tekortkomingen heeft geleid maar dat deze niet allemaal zijn opgelost. Bij de onderwerpen waar de Douane mee aan slag is gegaan, zijn in opzet grote stappen gezet maar mist nog in een aantal gevallen een verdere uitwerking in het bestaan. De resultaten per onderwerp uit hercontrole worden verder toegelicht in paragraaf 2.2.

Bij sommige onderwerpen waar tekortkomingen zijn geconstateerd tijdens de initiële audit, is door de Douane aangegeven dat er ten tijde van de hercontrole nog geen verbeteringen zijn gestart en gerealiseerd van materieel belang. In het verbeterrapport staat beschreven dat de eerste verbeteracties op die onderwerpen staan gepland voor kwartaal 4 in 2023 en kwartaal 1 in 2024. Deze onderwerpen zijn geen onderdeel van deze hercontrole en zijn in onderstaande tabel weergegeven als 'Niet Onderzocht' (NO). Voor deze onderwerpen blijven de bevindingen van de initiële audit staan.

Onderwerpen		Initiële Audit			Her-controle	
		O	B	W	O	B
1.	Doelbinding				NO	NO
2.	Noodzakelijkheid en rechtmatigheid politiegegevens				NO	NO
3.	Juistheid en volledigheid politiegegevens				NO	NO
4.	Bijzondere categorieën van politiegegevens					
5.	Geautomatiseerde individuele besluitvorming				NO	NO
6.	Onderscheid feiten en oordeel				NO	NO
7.	Autorisaties: aanwijzen functionarissen				NO	NO
8.	Onderscheid tussen verschillende categorieën van betrokkenen					
9.	Reikwijdte				NO	NO
10.	Gegevensbescherming door beveiliging en ontwerp				NO	NO
11.	Verwerker en verwerkersovereenkomst				NO	NO
12.	Geheimhoudingsplicht					
13.	Gegevensbeschermingseffectbeoordeling / DPIA				NO	NO
14.	Melding datalekken				NO	NO
15.	Gegevensbescherming door standaardinstellingen					
16.	Autorisaties en toegang tot politiegegevens				NO	NO
17.	Uitvoering van de dagelijkse politietaak				NO	NO

18. Geautomatiseerd vergelijken en in combinatie zoeken				NO	NO
19. Ondersteunende taken				NO	NO
20. Ter beschikking stellen (voor verdere verwerking)				NO	NO
21. Bewaartermijnen, verwijderen en vernietigen				NO	NO
22. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee				NO	NO
23. Doorgiften aan derde landen				NO	NO
24. Verstrekking aan derden structureel voor samenwerkingsverbanden				NO	NO
25. Rechtstreekse verstrekking					
26. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering				NO	NO
27. Register				NO	NO
28. Documentatie				NO	NO
29. Logging				NO	NO
30. Audits				NO	NO
31. Privacyfunctionaris					
32. Functionaris voor gegevensbescherming					

Overzicht conclusie per norm – organisatorische en technische beheersingsmaatregelen

1. Wijzigingenbeheer				NO	NO
2. Logische toegangs-beveiliging				NO	NO
3. Beheer van kwetsbaarheden (patch-management)				NO	NO
4. Cryptografie				NO	NO
5. Vulnerability scans en Penetratietesten					

Toelichting gebruikte kleuren:

	Voldoet aan de beheersingsmaatregel
	Voldoet deels aan de beheersingsmaatregel
	Voldoet niet aan de beheersingsmaatregel
	Niet onderzocht (NO) of niet van toepassing (NVT)

2.2 Bevindingen per onderwerp

2.2.1 Bijzondere categorieën van politiegegevens (4)

Wij hebben een Wpg kwaliteitshandboek aangetroffen waarmee in opzet het verwerken van bijzondere persoonsgegevens is beschreven als ook de manier waarop de Douane hiermee omgaat. Hiermee wordt voor de opzet aan de norm voldaan. Een beschrijving van of uitgevoerde controles hierop zijn niet aangetroffen waardoor het bestaan niet voldoet.

2.2.2 Onderscheid tussen verschillende categorieën van betrokkenen (8)

Wij hebben vastgesteld dat in het Wpg kwaliteitshandboek de verschillende categorieën van betrokkenen worden toegelicht. Ook hebben wij vastgesteld dat in het informatiesysteem en in de PV's onderscheid tussen de categorieën van betrokkenen wordt gemaakt waarmee in opzet en bestaan aan de norm wordt voldaan.

2.2.3 Geheimhoudingsplicht (12)

Wij hebben vastgesteld dat de Douane het laten vervallen van de BOA akte voor 5 van de 6 functies heeft geformaliseerd en borging is gevonden voor deze functies in de ministeriële regeling VOG-P. Hiermee is de eerdere bevinding en aanbeveling opgevolgd en wordt in opzet en bestaan aan de norm voldaan.

2.2.4 *Gegevensbescherming door standaardinstellingen (15)*

Wij hebben vastgesteld dat door diverse risicoanalyses aandacht aan gegevensbescherming is gegeven. De uitkomsten van de analyses zijn als input voor Autorisaties en Toegang tot politiegegevens gebruikt waarmee aan de norm wordt voldaan.

2.2.5 *Rechtstreekse verstrekking (25)*

Voor rechtstreekse verstrekkingen van politiegegevens is een proces beschreven en ingericht waarmee voor de opzet aan de norm wordt voldaan. Wij hebben vastgesteld dat periodiek aan de hand van zogenoemde viermaandsrapportages controles op uitgaande correspondentie worden uitgevoerd. De invulling en effectiviteit van dit proces blijkt niet uit het cyclisch ingerichte (interne) toezicht op de naleving van de Wpg door de PF en/of pFG waardoor voor het bestaan niet volledig aan de norm wordt voldaan.

2.2.6 *Privacyfunctionaris (31)*

Wij hebben vastgesteld dat de Douane per 8 februari 2023 de rol van privacy Officer heeft belegd waarmee in opzet aan de norm wordt voldaan. Een werkende cyclus van intern toezicht is niet aangetroffen. Een schriftelijke verslaglegging van doelen van het rechercheonderzoek (art 9), verstrekkingen, feitelijke of juridische redenen die ten grondslag liggen aan een afwijzing, inbreuk op de beveiliging van persoonsgegeven is niet aangetroffen. Een jaarlijks verslag van de bevindingen van de Privacyfunctionaris is niet aangetroffen waardoor niet aan de norm voor het bestaan wordt voldaan.

2.2.7 *Functionaris voor gegevensbescherming (32)*

Wij hebben vastgesteld dat een Functionaris voor gegevensbescherming is aangesteld waarmee in opzet aan de norm wordt voldaan. Toezicht door de Functionaris voor gegevensbescherming heeft niet plaatsgevonden. In 2023 is geen sprake van een werkend controle en toezichtsysteem specifiek voor de naleving van de Wpg. Het jaarlijkse toezicht door de pFG inclusief verslaglegging heeft niet plaatsgevonden. Hierdoor wordt voor het bestaan niet aan de norm voldaan.

2.2.8 *Vulnerability scans en penetratietesten (34)*

Wij hebben procesbeschrijvingen voor interne en externe security audits aangetroffen waarmee vulnerability scans en penetratietesten in opzet zijn beschreven. Hiermee wordt voor de opzet aan de norm voldaan. Ook hebben wij vastgesteld dat een pentest voor het Douane Fraude Bestrijding (DFB) systeem is uitgevoerd. Periodieke, volgens vastgesteld beleid en risicoanalyses, uitgevoerde vulnerability scans en pentesten op de systemen waarin politiegegevens verwerkt worden, zijn niet aangetroffen waardoor voor het bestaan niet aan de norm wordt voldaan.

3 Verantwoording onderzoek

3.1 Werkzaamheden en afbakening

3.1.1 Object van onderzoek

Het object van onderzoek van deze audit bestond uit de procedures en maatregelen die de Douane heeft getroffen naar aanleiding van de geconstateerde tekortkomingen tijdens de initiële Privacy Audit. De onderwerpen uit kwartaal 2 en 3 2023 die in deze audit per 1 december 2023 beoordeeld zijn omvatten:

4. Bijzondere categorieën van persoonsgegevens
8. Onderscheid tussen verschillende categorieën van betrokkenen
12. Geheimhoudingsplicht
15. Gegevensbescherming door standaardinstellingen
25. Rechtstreekse verstrekking
31. Privacy functionaris
32. Functionaris gegevensbescherming
34. Vulnerability scans en penetratietesten

Onderwerpen waar tijdens de initiële audit wel tekortkomingen zijn geconstateerd maar waarvan de Douane heeft aangegeven geen verbeteringen te hebben gerealiseerd, zijn geen object van onderzoek. De bevindingen op die onderwerpen tijdens de initiële audit blijven staan.

3.1.2 Criteria

Het onderzoek is uitgevoerd met het toetsingskader dat gebaseerd is op de in de Wpg en Bpg gestelde eisen evenals de NOREA Handreiking Privacy audit Wet politiegegevens (Wpg) voor Boa's.

Wij hebben uitsluitend onderzoek uitgevoerd naar de bij de initiële privacy audit als 'deels' of 'niet voldoende' in opzet en bestaan beoordeelde beheersingsmaatregelen én waarvan de organisatie heeft aangegeven verbeteringen te hebben gerealiseerd van materieel belang. Wij hebben geen onderzoek gedaan naar de bij de initiële audit niet beoordeelde normen en doen daar derhalve ook geen uitspraak over. Tevens doen wij geen uitspraak over de werking van de gerealiseerde verbetermaatregelen[2].

De (generieke) algehele beheersingsdoelstelling voor de privacy audit Wpg voor boa's is het voorzien in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens door boa's. Hiertoe heeft de organisatie beheersingsmaatregelen getroffen die in opzet en bestaan door de IT-auditor zijn getoetst. De IT-auditor heeft bij deze hercontrole gebruik gemaakt van de volgende criteria:

Opzet	De organisatie heeft de beheersingsmaatregen beschreven die, indien deze werken zoals beschreven, een redelijke mate van zekerheid bieden dat voorzien is aan de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens door boa's.
Bestaan	De organisatie heeft de beheersingsmaatregelen overeenkomstig de opzet daadwerkelijk geïmplementeerd en toegepast.

[2] De hercontrole heeft in beginsel alleen betrekking op opzet en bestaan, omdat de tijdspanne om een gewogen oordeel te geven over de werking in veel gevallen te kort zal zijn.

3.2 Gehanteerde Standaard

Deze opdracht is uitgevoerd volgens de Richtlijn voor assurance-opdrachten door IT-auditors (NOREA Richtlijn 3000D).

3.3 Verspreiding rapport

De opdrachtgever, 5.1.2e Woo Douane, is eigenaar van dit rapport en dient ingevolge artikel 33 2e lid van de Wpg een afschrift van de controleresultaten van deze hercontrole aan de Autoriteit persoonsgegevens te zenden.

De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. Voor openbaarmaking door het opdrachtgevende ministerie van door de ADR aan dit ministerie uitgebrachte rapporten gelden de voorschriften uit de Wet open overheid. De minister van Financiën stuurt elk halfjaar een overzicht van door de ADR uitgebrachte rapporten naar de Tweede Kamer.

4 Ondertekening

Den Haag, 26 februari 2024

5.1.2e Woo

Auditdienst Rijk

Bijlage | Managementreactie Douane

Bijlage | Managementreactie Douane

De Douane dankt de Auditdienst Rijk (hierna ADR) voor de hercontrole naar de voortgang op het verbeterrapport van de Wet politiegegevens (hierna Wpg) bij de Douane. Het betrof een controle op de uitgevoerde verbeteracties die de Douane gepland had voor het tweede en derde kwartaal van 2023.

De ADR komt op basis van deze hercontrole tot het oordeel dat: "bij de onderwerpen waar de Douane mee aan de slag is gegaan, zijn in opzet grote stappen gezet maar mist nog in een aantal gevallen een verdere uitwerking in het bestaan."

De Douane herkent zich in het oordeel van de ADR dat verdere verbeteracties nodig zijn – de Douane realiseert zich terdege dat er nog een grote inspanning gepleegd moet worden. De Douane continueert daarom haar inzet om de aanbevelingen van de ADR op te volgen. De bevindingen van deze hercontrole zien vooral op het aantoonbaar maken van het bestaan van de beheersmaatregelen en leiden tot aanpassing en aanvulling van het verbeterplan. Het is gebleken dat de uitwerking van de beheersmaatregelen meer tijd vergt dan in eerste instantie is ingeschat, daarom wordt een nieuwe planning van het verbeterplan opgesteld. Het aangevulde verbeterplan en de nieuwe planning zullen in maart van dit jaar gereed zijn. De inzet is daarbij om alle verbetermaatregelen (met uitzondering van de verbeteracties die samenhangen met systeemaanpassingen) in opzet én bestaan te realiseren voor het einde van 2024.

De verbeteracties die samenhangen met systeemaanpassingen zijn met voorrang in de IT-planning opgenomen. Daarbij speelt wel dat de Douane te maken heeft met een overvol IV-portfolio, wat noodzaakt tot reguliere prioritering van IT-werkzaamheden.

Door middel van jaarlijkse interne audits wordt de uitvoering van de maatregelen verder gemonitord.

5.1.2e Woo

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag